AMENDMENTS TO THE CLAIMS

1-17. **(Canceled)**

18. **(New)** An encrypted communication system comprising:

a first device; and

a second device, wherein

said first device includes:

a first data generation unit operable to encrypt a first key using a public key of said second device to generate first encrypted key data, and transmit the first encrypted key data to said second device;

a first decryption unit operable to receive, from said second device, second encrypted key data generated by said second device encrypting a third key using a public key of said first device, and decrypt the second encrypted key data using a private key of said first device to obtain a second key;

a first key generation unit operable to perform a predetermined operation using the first and second keys, generate a part of a result of the predetermined operation as a first encryption key and generate another part of the result as a first hash key; and

a first communication unit operable to encrypt first transmission data using the first encryption key to generate first encrypted data, apply a one-way operation to the first transmission data using the first hash key to calculate a first detection value for tamper detection to be performed on the first encrypted data by said second device, and transmit the first encrypted data and the first detection value to said second device, and

said second device includes:

a second data generation unit operable to encrypt the third key using the public key of said first device to generate the second encrypted key data, and transmit the second encrypted key data to said first device;

a second decryption unit operable to receive, from said first device, the first encrypted key

data generated by said first device encrypting the first key using the public key of said second device, and decrypt the first encrypted key data using a private key of said second device to obtain a fourth key;

a second key generation unit operable to perform the predetermined operation using the third and fourth keys, generate a part of a result of the predetermined operation as a second encryption key and generate another part of the result as a second hash key; and

a second communication unit operable to receive the first encrypted data and the first detection value, decrypt the first encrypted data using the second encryption key to generate second transmission data, apply a one-way operation to the second transmission data using the second hash key to calculate a second detection value, compare the first and second detection values, and when the first and second detection values match, recognize the second transmission data as valid, and when the first and second detection values do not match, recognize the second transmission data as invalid.

19. **(New)** A communication device for performing encrypted communication with another device using a shared key, comprising:

a data generation unit operable to encrypt a first key using a public key of the other device to generate first encrypted key data, and transmit the first encrypted key data to the other device;

a decryption unit operable to receive, from the other device, second encrypted key data generated by the other device encrypting a third key using a public key of the communication device, and decrypt the second encrypted key data using a private key of the communication device to obtain a second key;

a key generation unit operable to perform a predetermined operation using the first and second keys, generate a part of a result of the predetermined operation as a first encryption key and generate another part of the result as a first hash key; and

a communication unit operable to encrypt first transmission data using the first encryption key to generate first encrypted data, apply a one-way operation to the first transmission data using the first hash key to calculate a first detection value for tamper detection to be performed

on the first encrypted data by the other device, and transmit the first encrypted data and the first detection value to the other device.

20. **(New)** The communication device of claim 19, wherein

said key generation unit determines the result of the predetermined operation by performing, as the predetermined operation, an exclusive OR operation using the first and second keys.

21. **(New)** The communication device of claim 19, wherein

said data generation unit divides an operation result obtained by applying a one-way operation to a first seed value to generate a first coefficient and a first key, generates first encrypted key data by performing encryption using the first seed value and the first coefficient based on a public key of the other device, and transmits the first encrypted key data to the other device,

said decryption unit receives, from the other device, the second encrypted key data, generates a second seed value from the second encrypted key data based on a private key of the communication device, divides an operation result obtained by applying the one-way operation to the second seed value to generate a second coefficient and a second key, checks the second encrypted key data using the second coefficient, and when the second encrypted key data is correct, outputs the second key as a shared key identical to a third key of the other device, and

the other device

divides an operation result obtained by applying the one-way operation to a third seed value to generate a third coefficient and a third key, generates the second encrypted key data by performing encryption using the third seed value and the third coefficient based on a public key of the communication device, and transmits the second encrypted key data to the communication device,

receives, from the communication device, the first encrypted key data, generates a fourth seed value from the first encrypted key data based on a private key of the other device, divides an operation result obtained by applying the one-way operation to the fourth seed value to generate a

fourth coefficient and a fourth key, checks the first encrypted key data using the fourth coefficient, and when the first encrypted key data is correct, outputs the fourth key as a shared key identical to the first key,

generates a second encryption key based on the third and fourth keys, and

performs the encrypted communication with the communication device using the second encryption key.

22. **(New)** A method of performing encrypted communication with another device using a shared key, the method comprising:

encrypting, using a data generation unit, a first key using a public key of the other device to generate first encrypted key data, and transmitting the first encrypted key data to the other device;

receiving, using a decryption unit and from the other device, second encrypted key data generated by the other device encrypting a third key using a public key of the communication device, and decrypting the second encrypted key data using a private key of the communication device to obtain a second key;

performing, using a key generation unit, a predetermined operation using the first and second keys, generating a part of a result of the predetermined operation as a first encryption key and generating another part of the result as a first hash key; and

encrypting, using a communication unit, first transmission data using the first encryption key to generate first encrypted data, applying a one-way operation to the first transmission data using the first hash key to calculate a first detection value for tamper detection to be performed on the first encrypted data by the other device, and transmitting the first encrypted data and the first detection value to the other device.

23. **(New)** A computer program recorded on a computer-readable recording medium, the computer program being used for performing encrypted communication with another device using a shared key, the computer program causing a computer to execute:

encrypting a first key using a public key of the other device to generate first encrypted key data, and transmitting the first encrypted key data to the other device;

receiving, from the other device, second encrypted key data generated by the other device encrypting a third key using a public key of the communication device, and decrypting the second encrypted key data using a private key of the communication device to obtain a second key;

performing a predetermined operation using the first and second keys, generating a part of a result of the predetermined operation as a first encryption key and generating another part of the result as a first hash key; and

encrypting first transmission data using the first encryption key to generate first encrypted data, applying a one-way operation to the first transmission data using the first hash key to calculate a first detection value for tamper detection to be performed on the first encrypted data by the other device, and transmitting the first encrypted data and the first detection value to the other device.

24. **(New)** The encrypted communication system of Claim 18, wherein

the first encryption key and the first hash key are included in a hash calculation result that is generated by performing a hash calculation using the concatenated data generated by concatenating the first and second keys.

25. **(New)** The communication device of Claim 19, wherein

the first encryption key and the first hash key are included in a hash calculation result that is generated by performing a hash calculation using the concatenated data generated by concatenating the first and second keys.

26. **(New)** The method of Claim 22, wherein

the first encryption key and the first hash key are included in a hash calculation result that is generated by performing a hash calculation using the concatenated data generated by

concatenating the first and second keys.

27. **(New)** The computer program of Claim 23, wherein

the first encryption key and the first hash key are included in a hash calculation result that is generated by performing a hash calculation using the concatenated data generated by concatenating the first and second keys.

28. **(New)** The communication device of claim 21, wherein

a base element and the public key of the other device are defined in a group, the public key of the other device having been calculated by performing a power operation using the private key of the other device and the base element,

said data generation unit of the communication device divides the operation result obtained by applying the one-way operation to the first seed value which is a random number to generate the first coefficient and the first key, calculates the first element in the group by performing a power operation using the first coefficient and the base element, calculates a second element in the group by performing a power operation using the first coefficient and the public key of the other device, calculates a first verification value by performing a logical operation using the first seed value, the first element, and the second element, and outputs the first element and the first verification value as the first encrypted key data,

the other device acquires the first element and the first verification value as the first encrypted key data, calculates a third element in the group by performing a power operation using the private key of the other device and the first element, calculates a second verification value by performing the logical operation using the first verification value, the first element, and the third element, divides an operation result obtained by applying the one-way operation to the second verification value to generate a fourth efficient and a fourth key, compares an operation result of a power operation using the fourth coefficient and the base element, and the first element, and when the operation result and the first element match, recognizes the fourth key as the shared key identical to the first key,

the base element and the public key of the communication device are defined in the group, the public key of the communication device having been calculated by performing a power operation using the private key of the communication device and the base element,

the other device divides the operation result obtained by applying the one-way operation to the second seed value which is a random number to generate the third coefficient and the third key, calculates a fourth element in the group by performing a power operation using the third coefficient and the base element, calculates a fifth element in the group by performing a power operation using the third coefficient and the public key of the communication device, calculates a third verification value by performing the logical operation using the second seed value, the fourth element, and the fifth element, and outputs the fourth element and the third verification value as the second encrypted key data,

said decryption unit of the other device acquires the fourth element and the third verification value as the second encrypted key data, calculates a sixth element in the group by performing a power operation using the private key of the communication device and the fourth element, calculates a fourth verification value by performing the logical operation using the third verification value, the fourth element, and the sixth element, divides an operation result obtained by applying the one-way operation to the fourth verification value to generate the second efficient and the second key, compares an operation result of a power operation using the second coefficient and the base element, and the fourth element, and when the operation result and the fourth element match, recognizes the second key as a shared key.

29. **(New)** The communication device of claim 28, wherein

when P is a base point as the base element on an elliptic curve E as the group, x is the private key of the other device, $W = x*P$ is the public key of the other device, and "*" represents an operand indicating the power operation which is multiplication of a point on the elliptic curve E,

said data generation unit of the communication device

(a) generates the first seed value s which is a random number;

(b) calculates a hash value $G(s)$ of the first seed value s;

(c) divides the hash value $G(s)$ to generate the first coefficient a and the first key;

(d) calculates a point $R = a*P$ as the first element and a point $Q = a*W$ as the second element, on the elliptic curve E;

(e) performs an exclusive OR using the first seed value s and a hash value obtained by applying a hash function to a result of concatenating the points R and Q to obtain the first verification value v; and

(f) outputs the point R and the first verification value v as the first encrypted key data,

the other device

(g) acquires the point R and the first verification value v;

(h) calculates point $Q' = x*R$ as the third element on the elliptic curve E;

(i) performs an exclusive OR using the first verification value v and a hash value obtained by applying a hash function to a result of concatenating the points R and Q', to obtain the second verification value s';

(j) calculates a hash value $G(s')$ of the second verification value s';

(k) divides the hash value $G(s')$ to generate the fourth coefficient a' and the fourth key;

(l) judges whether $R = a'* P$ is established or not; and

(m) when judging that $R = a'*P$ is established, recognizes the fourth key as the shared key identical to the first key, and

when P is the base point as the base element on the elliptic curve E as the group, x is the private key of the communication device, $W = x*P$ is the public key of the communication device,

the other device

(a) generates the third seed value s which is a random number;

(b) calculates a hash value $G(s)$ of the third seed value s;

(c) divides the hash value $G(s)$ to generate the third coefficient a and the third key;

(d) calculates the point $R = a*P$ as the fourth element and the point $Q = a*W$ as the fifth element, on the elliptic curve E;

(e) performs an exclusive OR using the third seed value s and a hash value obtained by applying a hash function to a result of concatenating the points R and Q to obtain the third verification value v; and

(f) outputs the point R and the third verification value v,

the decryption unit of the communication device

(g) acquires the point R and the third verification value v;

(h) calculates the point $Q' = x*R$ as the sixth element on the elliptic curve E;

(i) performs an exclusive OR using the third verification value v and a hash value obtained by applying a hash function to a result of concatenating the points R and Q' to obtain the fourth verification value s';

(j) calculates a hash value $G(s')$ of the fourth verification value s';

(k) divides the hash value $G(s')$ to generate the second coefficient a' and the second key;

(l) judges whether $R = a'*P$ is established or not; and

(m) when judging that $R = a'*P$ is established, recognizes the fourth key as the shared key.

30. **(New)** The communication device of claim 19, wherein

said key generation unit, as the predetermined operation, concatenates the first and second keys to generate concatenated data, calculates a hash value for the concatenated data, and determines the hash value as the result of the operation.

31. **(New)** The communication device of claim 19, wherein

said communication unit includes:

a receiving subunit operable to receive, from the other device, second encrypted data generated by encrypting second transmission data using a second encryption key held by the other device, and a second detection value calculated for the second transmission data using a second hash key held by the other device;

a decryption subunit operable to decrypt the second encrypted data using the first encryption key to obtain plaintext data; and

a judging subunit operable to calculate a second hash value for the plaintext data using the second hash key, and judge whether the second hash value and the second detection value match, and

the communication device further includes a usage unit operable to use the plaintext data when the second hash value and the second detection value are judged to match, and to suppress use of the plaintext data when the second hash value and the second detection value are judged not to match.

32. **(New)** The communication device of claim 19 further comprising an authentication unit operable to authenticate the other device, using the first encryption key.

33. **(New)** The communication device of claim 32, wherein

the authentication unit (i) generates a first authentication value, encrypts the first authentication value using the first encryption key to generate a first encrypted value, and transmits the first encrypted value to the other device, and (ii) receives, from the other device, a second authentication value generated by decrypting the first encrypted value using a second encryption key held by the other device, and judges whether the first and second authentication values match, and

said communication unit performs communication with the other device when the authentication values are judged to match.

34. **(New)** The communication device of claim 33, wherein

the authentication unit receives, from the other device, a third encrypted value generated by encrypting a third authentication value using the second encryption key held by the other device,

decrypts the third encrypted value using the first encryption key to obtain a fourth authentication value, and transmits the fourth authentication value to the other device, and

said communication unit performs the communication when the other device judges the third and fourth authentication values to match.

35. **(New)** The encrypted communication system of claim 18, wherein

the first key generation unit, as the predetermined operation, concatenates the first and second keys to generate concatenated data, calculates a hash value for the concatenated data, and determines the hash value as the result of the operation.

36. **(New)** The encrypted communication system of claim 18, wherein

the first communication unit includes:

a receiving subunit operable to receive, from the second device, second encrypted data generated by encrypting second transmission data using a second encryption key held by the second device, and a second detection value calculated for the second transmission data using a second hash key held by the second device;

a decryption subunit operable to decrypt the second encrypted data using the first encryption key to obtain plaintext data; and

a judging subunit operable to calculate a first hash value for the plaintext data using the first hash key, and judge whether the first hash value and the second detection value match, and

the first communication device further includes a usage unit operable to use the plaintext data when the first hash value and the second detection value are judged to match, and to suppress use of the plaintext data when the first hash value and the second detection value are judged not to match.

37. **(New)** The encrypted communication system of claim 18, wherein

said first device further includes an authentication unit operable to authenticate said second device, using the first encryption key.

38. **(New)** The encrypted communication system of claim 37, wherein

the authentication unit (i) generates a first authentication value, encrypts the first authentication value using the first encryption key to generate a first encrypted value, and transmits the first encrypted value to the second device, and (ii) receives, from the second device, a second authentication value generated by decrypting the first encrypted value using a second encryption key held by the second device, and judges whether the first and second authentication values match, and

the first communication unit performs communication with the second device when the authentication values are judged to match.

39. **(New)** The encrypted communication system of claim 38, wherein

the authentication unit receives, from the second device, a third encrypted value generated by encrypting a third authentication value using the second encryption key held by the second device, decrypts the third encrypted value using the first encryption key to obtain a fourth authentication value, and transmits the fourth authentication value to the second device, and

the first communication unit performs the communication when the second device judges the third and fourth authentication values to match.